

Docket No. 218201US2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Koji CHIDA, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: METHOD, APPARATUS AND PROGRAM FOR QUANTITATIVE COMPETITION AND RECORDING
MEDIUM HAVING RECORDED THEREON THE PROGRAM

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY

APPLICATION NUMBER

MONTH/DAY/YEAR

Japan

2001-010327


January 18, 2001

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

jc997 U.S. PTO
10/050541
01/18/02

日本国特許庁
JAPAN PATENT OFFICE

1370714J
jc997 U.S. PTO
10/050541
01/18/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2001年 1月18日

出願番号

Application Number:

特願2001-010327

出願人

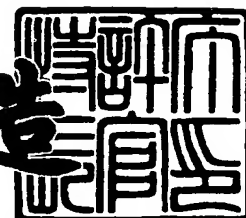
Applicant(s):

日本電信電話株式会社

2001年11月30日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3104947

【書類名】 特許願

【整理番号】 NTTH126706

【提出日】 平成13年 1月18日

【あて先】 特許庁長官殿

【国際特許分類】 G09C

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 千田 浩司

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 小林 邦生

【発明者】

【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内

【氏名】 森田 光

【特許出願人】

【識別番号】 000004226

【氏名又は名称】 日本電信電話株式会社

【代理人】

【識別番号】 100066153

【弁理士】

【氏名又は名称】 草野 卓

【選任した代理人】

【識別番号】 100100642

【弁理士】

【氏名又は名称】 稲垣 稔

【手数料の表示】

【予納台帳番号】 002897

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9806848

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 大小比較方法、その装置、そのプログラム及びその記録媒体

【特許請求の範囲】

【請求項 1】 掲示板装置と、複数のユーザの装置（以下ユーザ装置と記す）と、二つの大小比較装置（以下大小比較装置 A、大小比較装置 B、双方の場合は単に大小比較装置と記す）とを備え、

比較の対象となる整数値についてはあらかじめ上限 max および下限 min を定めていることを前提とし、全ユーザの意中の値からそれらの最小値およびその最小値を意中の値としたユーザだけが特定できる大小比較方法において、

掲示板装置は、ユーザ装置あるいは大小比較装置より受信した情報を即座に全て公開し、

各ユーザ i ($i = 1, 2, \dots, N$) は、 min 以上 max 以下の意中の値 V_i を決定してそのユーザ装置へ入力し、ユーザ装置は、 min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 max 以下に対応した情報は異なるような 2 系列の情報 s_i および t_i を作成し、 s_i あるいは t_i だけでは、 V_i に関する情報は全く分からないが s_i と t_i がそろえば V_i が分かるものとし、 s_i を大小比較装置 A に、 t_i を大小比較装置 B にそれぞれ秘密に送信し、

w 以下を意中の値としたユーザがいるかどうかの判定を、大小比較装置 A は全ユーザの情報 s_i から w に対応した情報 $s_{i,w}$ を取り出し、それらを決められた順序により並べたもの $Seq_{s,w} = s_{1,w} \parallel s_{2,w} \parallel \dots \parallel s_{N,w}$ (\parallel はデータの連結を表す) を作成し、大小比較装置 B は全ユーザの情報 t_i から w に対応した情報 $t_{i,w}$ を取り出し、それらを決められた順序により並べたもの $Seq_{t,w} = t_{1,w} \parallel t_{2,w} \parallel \dots \parallel t_{N,w}$ を作成し、 $Seq_{s,w}$ と $Seq_{t,w}$ を、それ自身の値を明かすことなく比較し、それらが異なっていれば w 以下を意中の値としたユーザがいると判定し、等しければ w 以下を意中の値としたユーザがいらないと判定し、その判定に基づき、 w の値を変更していくことで最小値を決定する、ことを特徴とする大小比較方法。

【請求項 2】 請求項 1 記載の方法において、

各ユーザ i のユーザ装置は、乱数 $R1_i$ 、 $R2_i$ を生成し、 $(R1_i, s_i)$

の組を大小比較装置Aに、 $(R2_i, t_i)$ の組を大小比較装置Bにそれぞれ秘密に送信し、

また、各組の連結 $R1_i \parallel s_i, R2_i \parallel t_i$ についてハッシュ関数 h によってハッシュ値 $H1_i = h(R1_i \parallel s_i)$, $H2_i = h(R2_i \parallel t_i)$ を計算し、それらを掲示板装置に送信し、

掲示板装置は $H1_i, H2_i$ ($i = 1, 2, \dots, N$) を全ユーザのコミットとして公開する

ことを特徴とする大小比較方法。

【請求項3】 請求項2記載の方法において、

大小比較装置は、整数値 w を共有し、大小比較装置Aは、 $Seq_{s,w}$ についてハッシュ関数 h によってハッシュ値 $HS_w = h(Seq_{s,w})$ を計算し、それを掲示板装置に送信し、

大小比較装置Bは、乱数 $Seq_{t,w}$ についてハッシュ関数 h によってハッシュ値 $HT_w = h(Seq_{t,w})$ を計算し、それを掲示板装置に送信し、

掲示板装置は、大小比較装置より受信した HS_w, HT_w を公開して比較し、それらが異なっていれば w 以下を意中の値としたユーザがいると判断し、等しければ w 以下を意中の値としたユーザがいないと判断し、 w を変更していくことで最小値を決定する

ことを特徴とする大小比較方法。

【請求項4】 請求項3記載の方法において、

大小比較装置は、掲示板装置より予め公開された素数 P ($P-1$ は大きな素数を約数に持つ) を記憶し、

大小比較装置は、整数値 w を選択して共有し、

大小比較装置Aは、乱数 RA_w を生成し、連結 $RA_w \parallel HS_w$ についてハッシュ関数 h によってハッシュ値 $HA_w = h(RA_w \parallel HS_w)$ を計算し、 $HS_w^{RA_w} \pmod{P}$ を計算し、それらの組 $(HA_w, HS_w^{RA_w} \pmod{P})$ を掲示板装置に送信し、

大小比較装置Bは、乱数 RB_w を生成し、連結 $RB_w \parallel HT_w$ についてハッシュ関数 h によってハッシュ値 $HB_w = h(RB_w \parallel HT_w)$ を計算し、 $HT_w^{RB_w}$

$(\text{mod } P)$ を計算し、それらの組 $(H B_w, H T_w^{RBw} (\text{mod } P))$ を掲示板装置に送信し、

次に大小比較装置 A は、 $(H T_w^{RBw})^{RAw} (\text{mod } P)$ を、大小比較装置 B は、 $(H S_w^{RAw})^{RBw} (\text{mod } P)$ をそれぞれ計算して、掲示板装置に送信し、

掲示板装置は、大小比較装置より受信した $(H T_w^{RBw})^{RAw} (\text{mod } P)$ 、 $(H S_w^{RAw})^{RBw} (\text{mod } P)$ を公開して比較し、それらが異なっていれば w 以下を意中の値としたユーザがいると判定し、等しければ w 以下を意中の値としたユーザがいらないと判定し、 w を変更していくことで最小値を決定することを特徴とする大小比較方法。

【請求項 5】 請求項 3 または 4 記載の方法において、

大小比較装置は、初期値 w を $(\text{max} + \text{min}) / 2$ 以下の最大の整数として共有し、 w 以下を意中の値としたユーザがいると判別されたときは max に w を代入し、そうでないときは min に $w + 1$ を代入して、 $\text{max} = \text{min}$ ($= \text{min value}$) となるまで判別を繰り返し、最小値 min value を求め、その過程を掲示板装置により逐次公開することを特徴とする大小比較方法。

【請求項 6】 請求項 3 又は 5 記載の方法において、

最小値 min value が公開された後、大小比較装置 A は、 $\text{Seq}_{s, \text{minvalue}}$ を、大小比較装置 B は、 $\text{Seq}_{t, \text{minvalue}}$ を掲示板装置に送信することを特徴とする大小比較方法。

【請求項 7】 請求項 4 又は 5 記載の方法において、

最小値 min value が公開された後、大小比較装置 A は、 $\text{Seq}_{s, \text{minvalue}}, R A_{\text{minvalue}}$ を、大小比較装置 B は、 $\text{Seq}_{t, \text{minvalue}}, R B_{\text{minvalue}}$ を掲示板装置に送信することを特徴とする大小比較方法。

【請求項 8】 請求項 1 ～ 7 の何れかに記載の方法において、

3 以上 M 個の大小比較装置 $A_j (j = 1, 2, \dots, M)$ が備えられ、各ユーザ $i (i = 1, 2, \dots, N)$ のユーザ装置は V_i が入力されると min 以上 V_i 未満に対応した情報は全て等しく、 V_i 以上 max 以下に対応した情報は全て異なるような M 系列の情報 $s_{ik} (k = 1, 2, \dots, M)$ を作成し、少なく

とも s_{ik} のうち2系列 s_{ia}, s_{ib} ($a \neq b$) がそろえば V_i が分かるものとし、
 s_{ik} を大小比較装置 A_k にそれぞれ秘密に送信し、

2個の大小比較装置で大小比較を行い、大小比較装置にトラブルが発生すると、他の正常な大小比較装置を用いてその比較動作を継続して行うことを特徴とする大小比較方法。

【請求項9】 請求項1～7の何れかに記載の方法において、

各ユーザ i ($i = 1, 2, \dots, N$) のユーザ装置は V_i が入力されると、 \min 以上 V_i 以下に対応した情報は異なり、 $V_i + 1$ 以上 \max 以下に対応した情報は等しいような2系列の情報 s_i および t_i を作成し、 s_i あるいは t_i だけでは、 V_i に関する情報は全く分からないが s_i と t_i がそろえば V_i が分かるものとし、 s_i を大小比較装置Aに、 t_i を大小比較装置Bにそれぞれ秘密に送信し、上記比較において異なっていれば w 以上を意中の値としたユーザがいると判断し、等しければ w 以上を意中の値としたユーザがいないと判断し、

全ユーザの意中の値からそれらの最大値およびそのユーザだけが特定することを特徴とする大小比較方法。

【請求項10】 請求項9記載の方法において、

各ユーザ i ($i = 1, 2, \dots, N$) のユーザ装置に V_i が入力されると、 \min 以上 V_i 以下に対応した情報は異なり、 $V_i + 1$ 以上 \max 以下に対応した情報は等しいような2系列の情報 s_i および t_i として、一方向性関数 F に対して $F^d(s_i) = F^d(t_i)$ ($d = 0, 1, \dots, V_i - \min$) かつ $F^e(s_i) \neq F^e(t_i)$ ($e = V_i - \min + 1, \dots, \max - \min$) を生成する(ここで例えば $F^3(s_i)$ は $F(F(F(s_i)))$ を表す)ことを特徴とする大小比較方法。

【請求項11】 請求項1～7の何れかに記載の方法において、

各ユーザ i ($i = 1, 2, \dots, N$) のユーザ装置は V_i が入力されると、 \min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 \max 以下に対応した情報は異なるような2系列の情報 s_i および t_i として一方向性関数 F に対して、 $F^d(s_i) \neq F^d(t_i)$ ($d = 0, 1, \dots, \max - V_i$) かつ $F^e(s_i) = F^e(t_i)$ ($e = \max - V_i + 1, \dots, \max - \min$) を生成する(ここで例えば $F^3(s)$ で $F(F(F(s)))$ を表す)

ことを特徴とする大小比較方法。

【請求項12】 大小比較方法に用いられるユーザ装置であって、

比較の対象となる整数値についての上限 max および下限 min が記憶された記憶部と、

min 以上 max 以下の意中の値 V_i を入力する入力手段と、

V_i と min , max が入力され、 min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 max 以下に対応した情報は異なる2系列の情報 s_i および t_i 、 min 以上 V_i 以下に対応した情報は異なり、 $V_i + 1$ 以上 max 以下に対応した情報は等しいような2系列の情報 s_i および t_i の一方を生成して出力する2系列生成部と、

s_i および t_i が入力され、これらに対する一方向性関数を演算して演算結果 $H1_i$, $H2_i$ を出力する一方向性関数演算部と、

s_i を大小比較装置Aへ、 t_i を大小比較装置Bへ、 $H1_i$ および $H2_i$ を掲示板装置へそれぞれ送信する送信部と
を具備するユーザ装置。

【請求項13】 大小比較方法に用いられる大小比較装置であって、

各ユーザ装置から送られた、比較の対象となる整数値についての上限 max から下限 min までの数よりなる系列を受信し、掲示板装置から送られた整数値 w を受信する受信部と、

受信した系列を記憶する記憶部と、

各ユーザの系列中から受信した w 番目の情報を入力して、これらの連結に対して一方向性関数を演算し、その演算結果を出力する一方向性関数演算部と、

上記一方向性関数演算結果を上記掲示板装置へ送信する送信部と
を具備する大小比較装置。

【請求項14】 大小比較方法に用いられるユーザ装置のコンピュータを、

比較の対象となる整数値についての上限 max 以下、下限 min 以上の意中の値 V_i を入力する入力手段、

min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 max 以下に対応した情報は異なる2系列の情報 s_i および t_i 、 min 以上 V_i 以下に対応した情報

は異なり、 $V_i + 1$ 以上 max 以下に対応した情報は等しいような 2 系列の情報 s_i および t_i の一方を生成する手段、

s_i および t_i に対しそれぞれ一方向性関数を演算して演算結果 $H1_i$, $H2_i$ を出力する手段、

s_i を大小比較装置 A へ、 t_i を大小比較装置 B へ、 $H1_i$ および $H2_i$ を掲示板装置へそれぞれ送信する手段、

として機能させるためのプログラム。

【請求項 15】 大小比較方法に用いられるユーザ装置のコンピュータを、比較の対象となる整数値についての上限 max 以下、下限 min 以上の意中の値 V_i を入力する入力手段、

min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 max 以下に対応した情報は異なる 2 系列の情報 s_i および t_i 、 min 以上 V_i 以下に対応した情報は異なり、 $V_i + 1$ 以上 max 以下に対応した情報は等しいような 2 系列の情報 s_i および t_i の一方を生成する手段、

s_i および t_i に対しそれぞれ一方向性関数を演算して演算結果 $H1_i$, $H2_i$ を出力する手段、

s_i を大小比較装置 A へ、 t_i を大小比較装置 B へ、 $H1_i$ および $H2_i$ を掲示板装置へそれぞれ送信する手段、

として機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、情報セキュリティ技術の応用技術であって、例えばインターネットなどによるオンライン上で、複数のユーザ（利用者）が意中の値を秘密に保持したまま比較し、最大値あるいは最小値と、それを意中の値としたユーザだけが特定される方法およびその装置に関するものである。

【0002】

【従来の技術】

大小比較がオンラインで実施される例として「電子入札方式」などがある。上記方式では、最大値あるいは最小値と、それを意中の値としたユーザは特定されるが、その他の情報は秘密に保持される技術が例えば

・小林, 森田, 「大小比較に一方方向性関数を用いた効率的な入札方式」, I S E C 99, などに示されている。また、

・H.Kikuchi, M.Harkavy, D.Tygar, “Multi-round anonymous auction protocols” In IEEE Workshop on Dependable and Real-Time E-Commerce System, 1998, では、ある数値に対してそれ以上あるいはそれ以下を意中の値としたユーザがいるかどうかだけが分かる方式を提案している。しかしながら最大値あるいは最小値を意中の値としたユーザが複数いる場合にそのユーザを特定できないことと、最大値あるいは最小値を意中の値としたユーザが2番目の数値を知り得てしまうという問題点があった。

【0003】

【発明が解決しようとする課題】

この発明の目的は複数のユーザが意中のものとした値の大小をオンラインで比較して、安全かつ高速に、これらの最大値あるいは最小値、更に必要に応じてそれを意中の値としたユーザだけが特定され、他は秘密が保持されるための方法およびその装置を提供することにある。

【0004】

【課題を解決するための手段】

比較の対象となる整数値についてはあらかじめ上限 \max および下限 \min を定めておく。なお、最大値、最小値のどちらを特定するかには本質的に変わりはないので、ここでは最小値を特定する場合のみを説明する。

各ユーザ i ($i = 1, 2, \dots, N$) は、 \min 以上 \max 以下の意中の値 V_i を決定した後、ユーザ装置により、 \min 以上 V_i 未満に対応した情報は等しく、 V_i 以上 \max 以下に対応した情報は異なるような2系列の情報 s_i および t_i を作成し、 s_i を大小比較装置 A に、 t_i を大小比較装置 B にそれぞれ秘密に送信する。 s_i あるいは t_i だけでは、 V_i に関する情報は全く分からないために、誰にもまた各大小比較装置にさえも V_i が知られることはない。

【0005】

全ユーザの意中の値に関する情報 s_i, t_i ($i = 1, 2, \dots, N$) がそろったら次に最小値を決定する。この手順は自由であるが、効率的な手法を以下に示す。まず $(\max + \min) / 2$ 以下の最大の整数 (これを w とする) 以下を意中の値としたユーザがいるかどうかの判定を、大小比較装置 A は全ユーザの情報 s_i から w に対応した情報 $s_{i,w}$ を取り出し、それらを決められた順序 (例えばユーザに予め番号が割り振られていてその番号順など) により並べたもの $\text{Seq}_{s,w} = s_{1,w} \parallel s_{2,w} \parallel \dots \parallel s_{N,w}$ (\parallel はデータの連結を表す) を作成し、大小比較装置 B は全ユーザの情報 t_i から w に対応した情報 $t_{i,w}$ を取り出し、それらを決められた順序により並べたもの $\text{Seq}_{t,w} = t_{1,w} \parallel t_{2,w} \parallel \dots \parallel t_{N,w}$ を作成し、 $\text{Seq}_{s,w}$ と $\text{Seq}_{t,w}$ を、一方向性関数や暗号関数などを用いてそれ自身の値を明かすことなく比較し、それらが異なっていれば w 以下を意中の値としたユーザがいると判定し、 \max に w を代入し、同様に $\text{Seq}_{s,w}, \text{Seq}_{t,w}$ を生成し、前記比較を行い等しければ w 以下を意中の値としたユーザがいないと判定し、 \min に $w+1$ を代入して、上記操作を $\min = \max (= \text{minvalue})$ となるまで繰り返すことで最小値 minvalue を決定する。

【0006】

最後に $\text{Seq}_{s,\text{minvalue}}, \text{Seq}_{t,\text{minvalue}}$ を公開して、誰もが最小値 minvalue を意中の値としたユーザを特定することができるようにする。

【0007】

【発明の実施の形態】

大小比較を行う際、上限の整数値 \max 、下限の整数値 \min 、大きな素数 P ($P-1$ は大きな素因子を約数に持つ、つまり離散対数問題をより所とする暗号方式の条件を満たすようにし) がすでに決められているものとする。

まず第1の実施形態として、2つの大小比較装置を用いて全ユーザの意中の値から最小値およびそれを意中の値としたユーザのみが特定できる方法を示す。次に第2の実施形態として、3つの大小比較装置を用いるが、そのうちの1つは大小比較の途中でシステムがダウンした場合に、全ユーザの出した意中の値から最小値およびそれを意中の値としたユーザのみを特定できる方法を示す。

第1の実施形態

まずはじめに、第1の実施形態における全体の位置付けを図1に示す。大小比較装置15A及び15B、掲示板装置19が設けられ、各ユーザ装置13-1～13-Nは図に示していない通信網を通じて大小比較装置15A及び15B、また掲示板装置19と通信することができ、大小比較装置15A及び15Bは掲示板装置19と通信することができる。

【0008】

なお番号16は掲示板装置21に対する閲覧情報を示す。また掲示板装置21にはデータベース23が接続されている。

ユーザ i ($i=1, 2, \dots, N$)は、 \min 以上 \max 以下の意中の整数値 V_i を定め、そのユーザ装置13- i はキーボードなどの入力手段30により入力する。ユーザ装置13- i の2系列生成部33は入力された V_i にもとづき2系列の情報 s_i と t_i とを生成する。 $s_i = \{s_{i,1}, s_{i,2}, \dots, s_{i,M}\}$, $t_i = \{t_{i,1}, t_{i,2}, \dots, t_{i,M}\}$ 、 M は \min から \max までのユーザが意中の値とすることができる値の数であり、ここで V_i が \min から v 番目とすると、 $s_{i,1} = t_{i,1}$, $s_{i,2} = t_{i,2}$, \dots , $s_{i,v-1} = t_{i,v-1}$, $s_{i,v} \neq t_{i,v}$, $s_{i,v+1} \neq t_{i,v+1}$, \dots , $s_{i,M} \neq t_{i,M}$ とする。つまり s_i と t_i は \min 以上 V_i 未満の対応した要素(情報)は互いに等しく、 V_i 以上 \max 以下の対応した要素は互いに異なる。これらは例えば図6に示すように予め決めたビット数からなる乱数を $V_i - \min = v - 1$ 個、 $a_1, a_2, \dots, a_{(v-1)}$ を生成し(S1)、 n を v とし(S2)、2個の乱数を生成し(S3)、この2個の乱数が等しくなければ(S4)、 n を+1し(S5)、 n が \max 以上でなければステップS3に戻り(S6)、ステップS4で2つの乱数が等しければステップS3に戻り、ステップS6で n が \max 以上であればステップS7に移り、 $a_1, \dots, a_{(v-1)}$ を $s_{i,1}, s_{i,2}, \dots, s_{i,(v-1)}$ と $t_{i,1}, t_{i,2}, \dots, t_{i,(v-1)}$ とにし、これらに対し各2個ずつ発生した乱数を1個ずつ順次振分けて、残りの $s_{i,v}, \dots, s_{i,M}$ と $t_{i,v}, \dots, t_{i,M}$ とする。

【0009】

乱数生成部31から乱数 $R1_i, R2_i$ を生成し、 $(s_i, R1_i)$ の組を大小比

較装置15Aに、 $(t_i, R2_i)$ の組を大小比較装置15Bにそれぞれ秘密に、例えば暗号化部34で暗号化して送信する(この暗号化関数をDとする)。また、ハッシュ関数演算部35で各組の連結 $s_i \parallel R1_i, t_i \parallel R2_i$ についてハッシュ関数 h によってハッシュ値 $H1_i = h(s_i \parallel R1_i), H2_i = h(t_i \parallel R2_i)$ を計算し、それらを掲示板装置19に送信する。なお、 max, min 2系列 s_i, t_i 、乱数 $R1_i, R2_i, V_i$ は記憶部32に記憶され、各情報の大小比較装置15A, 15Bや掲示板装置19への送信は送信部36が行う。記憶部32に対する読み書き、各部に対する動作指示は制御部37により行う。このユーザ装置13-iはコンピュータによりプログラムを実行させて機能させるように構成してもよい。

【0010】

各ユーザ i はハッシュ値 $H1_i$ および $H2_i$ を掲示板装置19に送信し、その値が公開されることで V_i をコミットしたことになる。つまり V_i を明かすことなく、 V_i を意中の値としたことを登録したことになる。これにより、以降意中の値を変更不可能とするとともに、もしなんらかの理由で自分の意中の値より大きい値が最小値となったときは、 $s_i, R1_i, t_i, R2_i$ を公開することで自分の意中の値が最小値であることを示すことができる。また、乱数 $R1_i, R2_i$ を連結させているのは、 $H1_i = h(s_i), H2_i = h(t_i)$ とすると s_i あるいは t_i を知っているともう一方の値もあたりがつけやすくなるケースにも対応するため(s_i, t_i を知れば V_i が分かる)、大小比較装置15A, 15Bに対しても秘密を高めるためであり、乱数 $R1_i, R2_i$ を省略してもよい。

【0011】

大小比較装置15A, 15Bは図3、図4に示すように受信部40に受信された各ユーザ装置13-1~13-Nからの情報系列 $s_1 \sim s_N, t_1 \sim t_N$ はそれぞれ記憶部41に格納され、また受信した乱数 $R1_1 \sim R1_N, R2_1 \sim R2_N$ も格納される。記憶部41には前述した大きな素数 P も格納されてある。

全てのユーザ装置13-1~13-Nから情報系列 s_i, t_i 、乱数 $R1_i, R2_i$ 、ハッシュ値 $H1_i, H2_i$ が送信されると、例えば掲示板装置19から、 $(max + min) / 2$ 以下の最大の整数を初期値 w として大小比較装置15A,

15Bに送信され、 w が大小比較装置15A、15Bの受信部40に受信されると、大小比較装置15Aは、図3に示すように乱数生成部42から乱数 RA_w を生成し、全ユーザ装置から受信した s_i の w に対応した情報 $s_{i,w}$ を記憶部41から取り出しそれらをユーザ1、ユーザ2、…、ユーザNの順に並べたもの $Seq_{s,w} = s_{1,w} \parallel s_{2,w} \parallel \dots \parallel s_{N,w}$ を作成し、ハッシュ関数演算部43でハッシュ関数 h によって $Seq_{s,w}$ に対するハッシュ値 $HS_w = h(Seq_{s,w})$ および $RA_w \parallel HS_w$ に対するハッシュ値 $HA_w = h(RA_w \parallel HS_w)$ を計算し、その HS_w と乱数 RA_w をべき乗剰余演算部44に入力して $HS_w^{RA_w} \pmod{P}$ を計算し、それら $(HA_w, HS_w^{RA_w} \pmod{P})$ の組を掲示板装置19に送信部45より送信する。

【0012】

大小比較装置15Bは図4に示すように乱数生成部42、乱数 RB_w を生成し、全ユーザ装置から受信した t_i の w に対応した情報 $t_{i,w}$ を記憶部41から取り出し、それらをユーザ1、ユーザ2、…、ユーザNの順に並べたもの $Seq_{t,w} = t_{1,w} \parallel t_{2,w} \parallel \dots \parallel t_{N,w}$ を作成し、ハッシュ関数演算部43に入力してハッシュ関数 h によって $Seq_{t,w}$ に対するハッシュ値 $HT_w = h(Seq_{t,w})$ および $RB_w \parallel HT_w$ に対するハッシュ値 $HB_w = h(RB_w \parallel HT_w)$ を計算し、 HT_w と RB_w をべき乗剰余演算部44に入力して $HT_w^{RB_w} \pmod{P}$ を計算し、それら $(HB_w, HT_w^{RB_w} \pmod{P})$ の組を掲示板装置19に送信部45より送信する。

【0013】

次に大小比較装置15Aは、掲示板装置19より公開された $HT_w^{RB_w} \pmod{P}$ をべき乗剰余演算部44に閲覧入力して、 $(HT_w^{RB_w})^{RA_w} \pmod{P}$ を計算し、その計算結果を掲示板装置19に送信する。大小比較装置15Bも同様に、掲示板装置19より公開された $HS_w^{RA_w} \pmod{P}$ をべき乗剰余演算部44に閲覧入力して $(HS_w^{RA_w})^{RB_w} \pmod{P}$ を計算し、その結果を掲示板装置19に送信する。

HS_w と HT_w が等しければ、掲示板装置19に送信された $(HT_w^{RB_w})^{RA_w} \pmod{P}$ と $(HS_w^{RA_w})^{RB_w} \pmod{P}$ は等しく、また P が大きな素数であ

り、かつ $P-1$ は大きな素因子を約数にもつから、 HS_w と HT_w が異なり ($HT_w^{RBw} \cdot RAW \pmod{P}$) と ($HS_w^{RAW} \cdot RBw \pmod{P}$) が等しくなる可能性は無視できるほど小さいことから、($HT_w^{RBw} \cdot RAW \pmod{P}$) と ($HS_w^{RAW} \cdot RBw \pmod{P}$) が等しければ $s_{1,w} = t_{1,w}$, $s_{2,w} = t_{2,w}$, ..., $s_{N,w} = t_{N,w}$ であるから、 $w+1$ 以上が最小値ということになり、異なれば w 以下が最小値ということが圧倒的確率で分かる。掲示板装置 19 はこのことを判定し、もし等しければ min に $w+1$ を代入し、異なれば max に w を代入して上記操作を繰り返す。以上のことを繰り返すことにより、およそ $\log(max-min)$ 回で $max = min (= minvalue)$ となる。この $minvalue$ が最小値となる。この過程を図 5 に示す。つまりまず $(max+min)/2$ 以下の最大の整数を w としてその w について図 3、図 4 を参照して説明したように、大小比較装置 15A、15B にて HA_w , $HS_w^{RAW \pmod{P}}$, HB_w , $HT_w^{RBw \pmod{P}}$ をそれぞれ求め、更に ($HT_w^{RBw} \cdot RAW \pmod{P}$), ($HS_w^{RAW} \cdot RBw \pmod{P}$) をそれぞれ計算し (s1)、この計算結果が一致しているかを調べ (s2)、一致していれば $w+1$ を min とし (s3)、 $max = min$ になったかを調べ (s4)、なっていないければステップ s1 に戻り、ステップ s2 で一致していなければ、 w を max としてステップ s4 に移る (s5)。ステップ s4 で max と min とが等しければ、その min を最小値 ($minvalue$)、つまりユーザ 11-1 ~ 11-N がそれぞれ意中の値 $V_1 \sim V_N$ として、コミットしたもののうちの最小値が求まったことになる。

【0014】

この最小値 $minvalue$ が分かった後、大小比較装置 15A、15B はその最小値と対応する、 $Seq_{s,minvalue}$, $RA_{minvalue}$, $Seq_{t,minvalue}$, $RB_{minvalue}$ を掲示板装置 19 に送信することにより、全ユーザ 11-1 ~ 11-N は、それら 2 系列に対して対応する部分 $s_{j,w} \neq t_{j,w}$ と異なる情報が入った j 番目の部分に該当するユーザが最小値を意中の値としたと特定できる。 $Seq_{s,w}$, $Seq_{t,w}$ の配列順が知られていれば、前記異なる j 番目に該当するユーザ j が意中のものとした値 V_j が最小値であることを特定できる。

【0015】

最後に不正がなかったことを確認するため、大小比較装置 15A, 15B は最小値を意中の値としたユーザ j の $R1_j, s_j, R2_j, t_j$ を掲示板装置 19 に送信する。全ユーザは掲示板装置 19 より公開されたコミットとの対応を確認することができる。つまり、 $R1_j, s_j, R2_j, t_j$ の公開によりユーザ j は自身が意中の値としたものが最小となったことを知ることができ、また全てのユーザは、そのユーザ装置により、 $h(s_j \parallel R1_j)$ 及び $h(t_j \parallel R2_j)$ を演算し、これらがユーザ j がコミットした $H1_j$ 及び $H2_j$ とそれぞれ一致することを確認して、正しい操作（大小比較）が行われたことを知ることができる。なお $Seq_{s,w}, Seq_{t,w}$ の配列順とユーザとの関係が公開されていない場合には、 $R1_j, s_j, R2_j, t_j$ を公開した時点で、最小値を意中の値としたユーザ j が特定される。

【0016】

なお仮に HT_w を知ったものが HS_w を推定でき、それが正しいければ他のユーザの意中の値を知ることができるが、 P が大きな素数であり、かつ $P-1$ は大きな素因子を約数にもつようにされているため $HS_w^{RA_w}$ の RA_w を求めることが困難であるため、その HS_w が真に正しいものか知ることができない。従って他のユーザが意中の値を知ることとはできない。

また大小比較装置 15A, 15B において乱数 RA_w, RB_w を省略してもよいが、 RA_w, RB_w を用い、最後に、 $RA_{minvalue}, RB_{minvalue}$ を公開することにより、これらと $Seq_{s,minvalue}, Seq_{t,minvalue}$ を用いることにより、大小比較処理が正しく行われたかを確認することができる。

【0017】

大小比較装置 15A, 15B においてはその記憶部 41 に対する読み書き、受信情報の処理、各送信情報を対応する装置へ送信部 45 により送信させ、その他の各部の動作をさせることなどを制御部 46 で行う。この大小比較装置 15A, 15B もコンピュータによりプログラムを実行させて機能させることもできる。

掲示板装置 19 はその機能構成を特に図に示さなかったが、各ユーザ装置、大小比較装置 15A, 15B との送受信部を備え、受信された情報をデータベース 23 に格納し、閲覧要求があれば、対応する情報をデータベース 23 が読み出し

て、要求元へ送信し、また図5に示した処理とその実行に必要な送受信を行う。
この掲示板装置19もコンピュータによりプログラムを実行させて機能させるようにすることもできる。

第2の実施形態

ユーザ i ($i=1, 2, \dots, N$) は、 \min 以上 \max 以下の意中の整数値 V_i を定め、ユーザ装置により \min 以上 V_i 未満に対応した情報は全て等しく、 V_i 以上 \max 以下に対応した情報は全て異なるような3系列の情報 s_i, t_i, u_i を作成し、乱数 $R1_i, R2_i, R3_i$ を生成し、 $(s_i, R1_i)$ の組を大小比較装置Aに、 $(t_i, R2_i)$ の組を大小比較装置Bに、 $(u_i, R3_i)$ の組を大小比較装置Cに、それぞれ秘密に送信する。また、各組の連結 $s_i \parallel R1_i, t_i \parallel R2_i, u_i \parallel R3_i$ についてハッシュ関数 h によってハッシュ値 $H1_i = h(s_i \parallel R1_i), H2_i = h(t_i \parallel R2_i), H3_i = h(u_i \parallel R3_i)$ を計算し、それらを掲示板装置19に送信する。

【0018】

各ユーザ i は $H1_i$ および $H2_i$ および $H3_i$ を掲示板装置に送信し、その値が公開されることで V_i をコミットしたことになる。これにより、以降意中の値を変更不可能とするとともに、もしなんらかの理由で自分の意中の値より大きい値が最小値となったときは、 $(s_i, R1_i), (t_i, R2_i), (u_i, R3_i)$ の少なくとも2組を公開することで自分の意中の値が最小値であることを示すことができる。

以降、大小比較装置は2つで充分であるから、その2つを大小比較装置AおよびBとする。

【0019】

前述と同様に大小比較装置は、まず初期値 w を $(\max + \min) / 2$ 以下の最大の整数とし、大小比較装置Aは、乱数 RA_w を生成し、全ユーザ装置から受信した s_i の w に対応した情報 $s_{i,w}$ を取り出し、それらをユーザ1, ユーザ2, ..., ユーザ N の順に並べたもの $Seq_{s,w} = s_{1,w} \parallel s_{2,w} \parallel \dots \parallel s_{N,w}$ を作成し、ハッシュ関数 h によってハッシュ値 $HS_w = h(Seq_{s,w})$ および $HA_w = h(RA_w \parallel HS_w)$ および $HS_w^{RA_w} \pmod{P}$ を計算し、それら $(HA_w$

, $HS_w^{RAW} \pmod{P}$) の組を掲示板装置に送信する。大小比較装置 B は、乱数 RB_w を生成し、全ユーザ装置から受信した t_i の w に対応した情報 $t_{i,w}$ を取り出し、それらをユーザ 1, ユーザ 2, ..., ユーザ N の順に並べたもの $Seq_{t,w} = t_{1,w} \parallel t_{2,w} \parallel \dots \parallel t_{N,w}$ を作成し、ハッシュ関数 h によってハッシュ値 $HT_w = h(Seq_{t,w})$ および $HB_w = h(RB_w \parallel HT_w)$ および $HT_w^{RBw} \pmod{P}$ を計算し、それら $(HB_w, HT_w^{RBw} \pmod{P})$ の組を掲示板装置に送信する。

【0020】

次に大小比較装置 A は、掲示板装置より公開された $HT_w^{RBw} \pmod{P}$ を用いて、 $(HT_w^{RBw})^{RAW} \pmod{P}$ を計算し、それを掲示板装置に送信し、大小比較装置 B は、掲示板装置より公開された $HS_w^{RAW} \pmod{P}$ を用いて、 $(HS_w^{RAW})^{RBw} \pmod{P}$ を計算し、それを掲示板装置に送信する。

HS_w と HT_w が等しければ $(HT_w^{RBw})^{RAW} \pmod{P}$ と $(HS_w^{RAW})^{RBw} \pmod{P}$ は等しく、また P が大きな素数であり、かつ $P-1$ は大きな素因子を約数にもつから、 HS_w と HT_w が異なり $(HT_w^{RBw})^{RAW} \pmod{P}$ と $(HS_w^{RAW})^{RBw} \pmod{P}$ が等しくなる可能性は無視できるほど小さいことから、 $(HT_w^{RBw})^{RAW} \pmod{P}$ と $(HS_w^{RAW})^{RBw} \pmod{P}$ が等しければ $w+1$ 以上が最小値ということになり、異なれば w 以下が最小値ということが圧倒的確率で分かる。もし等しければ \min に $w+1$ を代入し、異なれば \max に w を代入して上記操作を繰り返すことにより、およそ $\log(\max - \min)$ 回で $\max = \min (= \minvalue)$ となる。この \minvalue が最小値となる。

【0021】

最小値 \minvalue が分かった後、大小比較装置は、 $Seq_{s,\minvalue}$, RA_{\minvalue} , $Seq_{t,\minvalue}$, RB_{\minvalue} を掲示板装置に送信することで、全ユーザは、それら 2 系列に対して異なる情報が入った部分に該当するユーザが最小値を意中の値としたユーザ j であるということを特定できる。

上記過程で、トラブルにより一方の大小比較装置、例えば B のシステムがダウンしたとする。しかし、大小比較装置 B のもつ情報と大小比較装置 C のもつ情報は本質的に同じであるから、そのまま大小比較装置 B の操作を大小比較装置 C が

引き継ぐことができる。

【0022】

最後に不正がなかったことを確認するため、大小比較装置は最小値を意中の値としたユーザ j の $R1_j, s_j, R3_j, u_j$ を掲示板装置に送信することで、全ユーザは掲示板装置より公開されたコミットとの対応を確認することができる。このように大小比較装置を更に多く設け、それに応じて情報系列の数を増加して同様に処理することにより、大小比較装置がトラブルになりシステムダウンした場合の安全性を高くすることもできる。

上述したことから理解できるように、各大小比較装置 15A, 15B は各ユーザ装置から受信した情報が正しいものであるかを掲示板装置 19 の対応公開情報 $H1_i, H2_i$ により検証することができる。また大小比較装置 15A, 15B の両者で $R1_i, s_i, R2_i, t_i$ を公開することにより、ユーザ i の意中の値 V_i が確かなものであることを検証することができる。

【0023】

大小比較装置 15A, 15B は $Seq_{s,minvalue}, Seq_{t,minvalue}$ を掲示板装置 19 に送信して公開した後、必要に応じて $Seq_{s,z}, Seq_{t,z}$ ($z = min, min+1, \dots, minvalue$) のうち大小比較処理に用いられたものを掲示板装置 19 へ送信し、 $minvalue$ が正しいものであることを明らかにしてもよい。

上述においては大小比較装置 15A, 15B で作成した $Seq_{s,w}, Seq_{t,w}$ をそれ自身の値を明かすことなく、比較するために一方向性関数を用いたが、例えば同一の暗号鍵で、同一の暗号演算を $Seq_{s,w}, Seq_{t,w}$ に対して、その結果を掲示板装置 19 へ送信して比較を行ってもよい。

【0024】

この発明では、要は、大小比較装置 15A, 15B において、 w に対応した情報 $s_{i,w}, t_{i,w}$ をそれぞれ取出し、それらを決められた順序に並べたもの $Seq_{s,w}$ と $Seq_{t,w}$ を作り、これらを明かすことなく比較して、異なるか等しいかにより、 w 以下（最大値を求める場合は w 以上）に意中の値としたユーザがいるかを判定し、その判定結果にもとづき、 w を変更すればよい。 HS_w と HT_w とを比較

して、上記判定をしてもよい。乱数 $R1_i$, $R2_i$ は安全性を高めたのであり、必ずしも用いなくてもよい。従って $H1_i = h(s_i)$, $H2_i = h(t_i)$ として掲示板装置へ送信してもよい。

【0025】

2系列情報 s_i , t_i としては例えば最小値を求める場合は一方向性関数 F に対して、 $F^d(s_i) \neq F^d(t_i)$ 、($d=0, 1, \dots, \max - V_i$) かつ $F^e(s_i) = F^e(t_i)$ 、($e = \max - V_i + 1, \dots, \max - \min$) となるようなものにしてもよい。ここで例えば $F^3(s_i)$ は $F(F(F(s_i)))$ を表わす。情報系列 s_i は

$$s_i = \{s_{i1} = F^{\max - \min}(s_i), s_{i2} = F^{\max - \min - 1}(s_i), \dots, F^{\max - V_i + 1}(s_i), F^{\max - V_i}(s_i), \dots, s_{iM-1} = F(s_i), s_{iM} = s_i\}$$

となる。つまり情報系列の順番が小さい方が最も多く関数演算される。最大値を求める場合も同様にこのように求めてもよい。このように関数値を用いると $\max - \min$ の数が多くなっても各系列の1つの情報のビット数は一定であるが、乱数を用いる場合は、用いる乱数のビット数を多くする必要があり、伝送や処理が大変になる。

【0026】

上述においては各ユーザの意中の値 V_i の最小値を決定したが、最大値の決定も同様に行うことができる。この場合は2系列情報 s_i と t_i としては、 \min 以上 V_i 以下に対応した情報は s_i と t_i とで異なり、 $V_i + 1$ 以上 \max 以下に対応した情報は s_i と t_i とで等しいようにする。また各選択された w についての $Seq_{s,w}$ と $Seq_{t,w}$ の比較、 $HS_w = h(Seq_{s,w})$ と $HT_w = h(Seq_{t,w})$ の比較、 $(HT_w^{RBW})^{RAW} \bmod P$ と $(HS_w^{RAW})^{RBW} \bmod P$ の比較において異なっていれば w 以上を意中の値としたユーザがいると判断し、等しければ w 以上を意中の値としたユーザがいらないと判断し、等しい場合は w を \max とし異なっていれば、 $w + 1$ を \min として、同様の処理を繰り返せばよい。

【0027】

w の決定は先に述べたようにすると効率的に最小値又は最大値を求めることができるが、 w を例えば \min 又は \max から順次変化させて大小比較を行っても

よい。更に1つの大小比較装置が最初のwを決定し、wを掲示板装置19を介して他の大小比較装置へ送り、掲示板装置19から必要な情報を受け取って、図5に示した処理を行ってもよい。

【0028】

【発明の効果】

以上述べたようにこの発明によれば、ユーザは意中の値に関する情報を1回だけ各大小比較装置および掲示板装置に送信するだけで、高速に最大値あるいは最小値とを特定でき、必要に応じてそれを意中の値としたユーザのみが特定できる、秘匿性の高い大小比較が実現できる。

【図面の簡単な説明】

【図1】

第1の実施形態の全体のシステム構成例を示す図。

【図2】

ユーザ装置のおもな機能構成例を示す図。

【図3】

大小比較装置15Aのおもな機能構成例を示す図。

【図4】

大小比較装置15Bのおもな機能構成例を示す図。

【図5】

最小値を特定するための流れ図。

【図6】

図2中の2系列生成部33の処理手順の例を示す図。

【書類名】 図面

【図1】

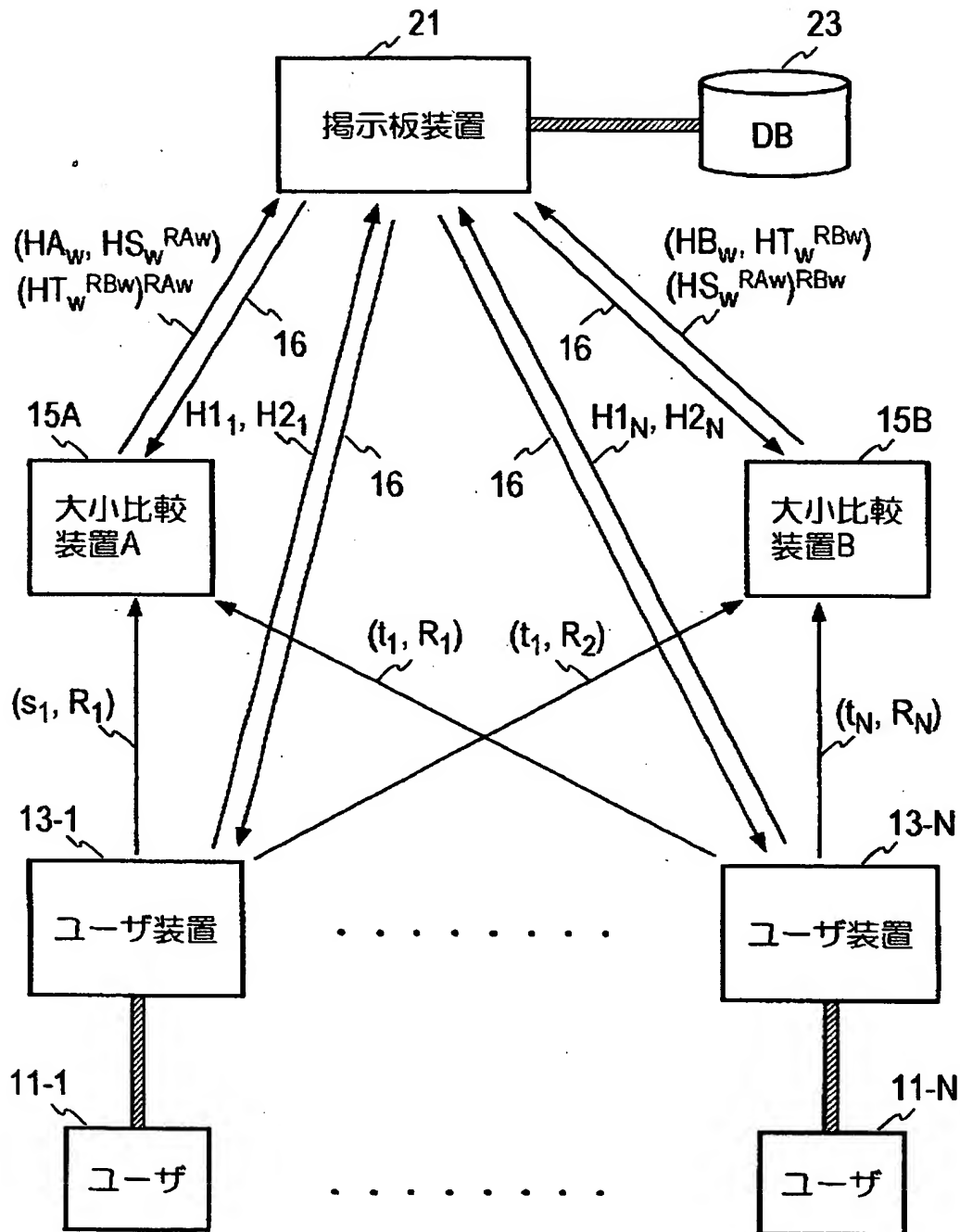


図1

【図 2】

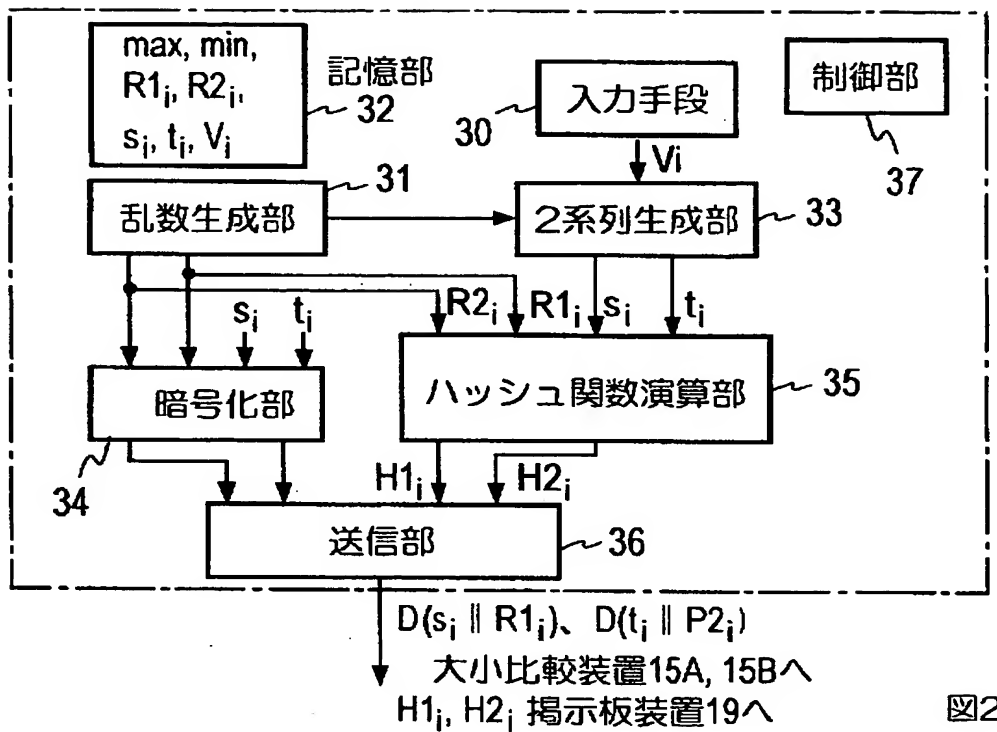


図2

【図 3】

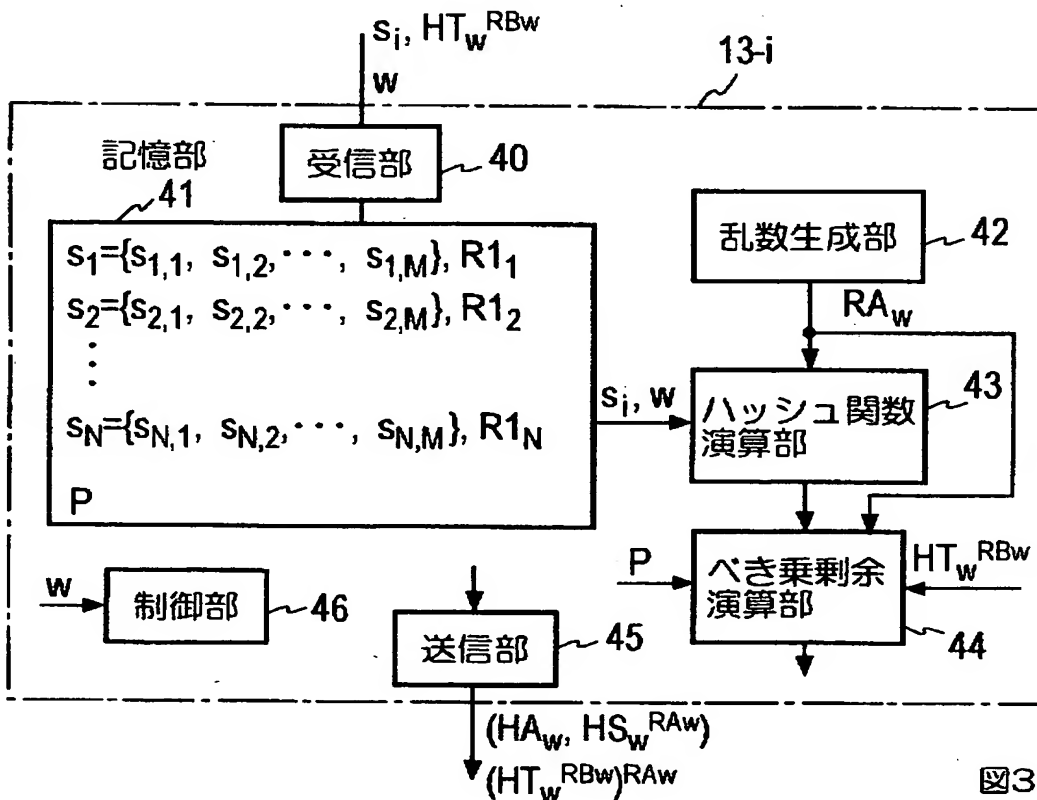


図3

【図 4】

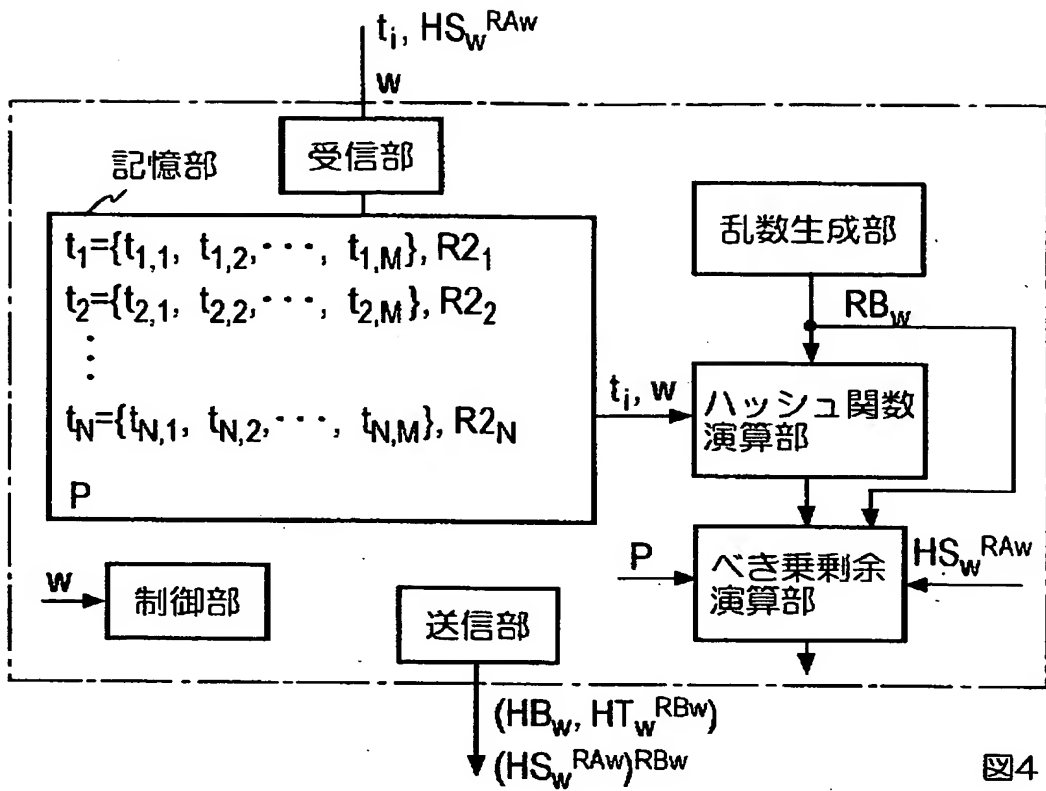


図4

【図 5】

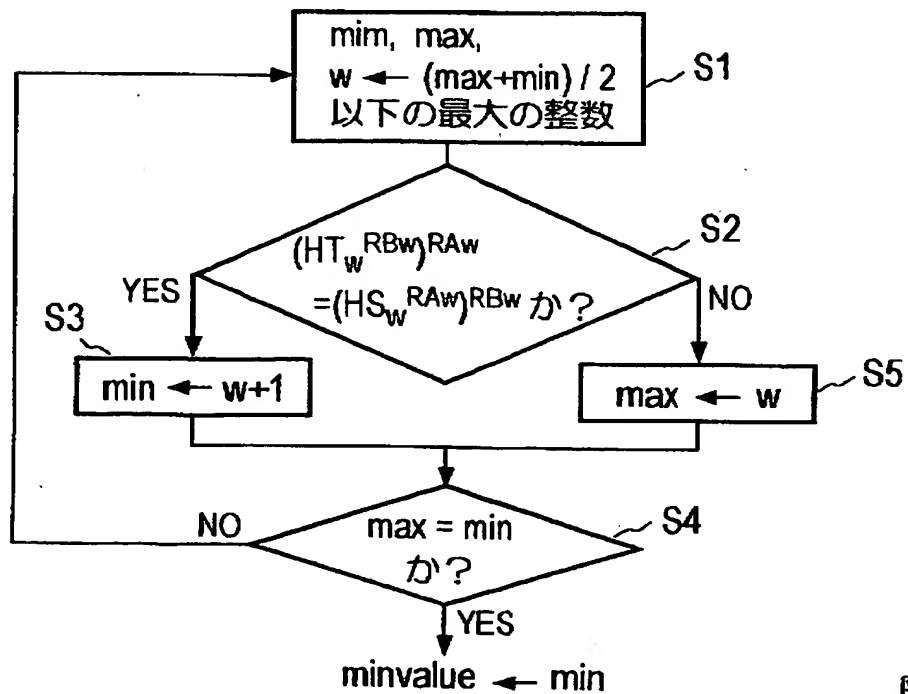


図5

【図6】

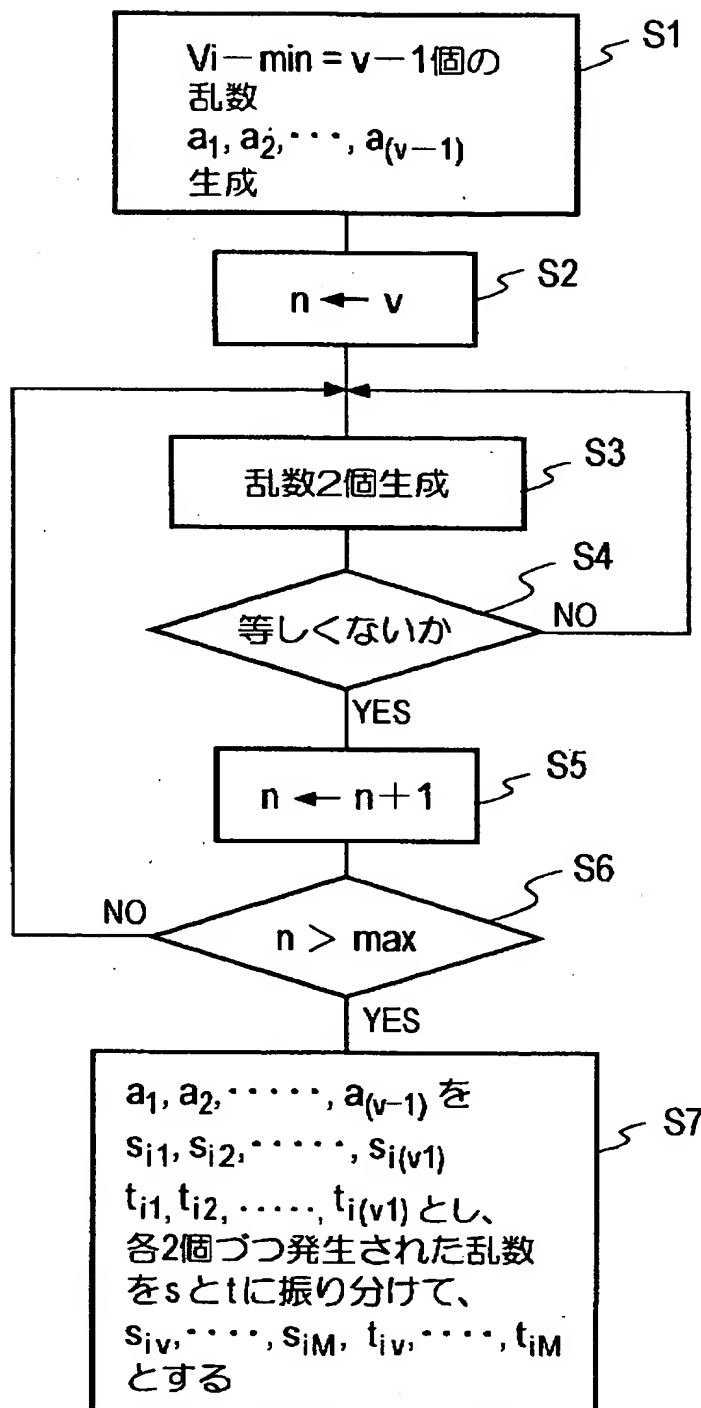


図6

【書類名】 要約書

【要約】

【課題】 競争入札に用いられ、ユーザは1回だけ入札値 V_i を送る。

【解決手段】 入札最小値 \min から最大値 \max まで各入札可能値に番号1, 2, ..., Mを付け、各ユーザ i は入札値 V_i に対し、 $s_i = \{s_{i1}, s_{i2}, \dots, s_{iM}\}$ 、 $t_i = \{t_{i1}, t_{i2}, \dots, t_{iM}\}$ 、 $s_{i1} = t_{i1}, \dots, s_{i,v-1} = t_{i,v-1}, s_{iv} \neq t_{iv}, \dots, s_{iM} \neq t_{iM}$ なる2系列を作り（ v は V_i の番号）、 s_i と t_i を大小比較装置15Aと15Bへそれぞれ秘密に送り、そのハッシュ値 $H1_i = h(s_i)$ 、 $H2_i = h(t_i)$ を掲示板21へ送り、大小比較装置15A、15Bは番号 w と対応して $s_1 \sim s_N$ から、各 s_{iw} 、 $t_1 \sim t_N$ から各 t_{iw} を取出し、 N 個の s_{iw} の連結 $Seq_{s,w}$ と N 個の t_{iw} の連結 $Seq_{t,w}$ を作り、これらを一方方向性関数を用いて、その各値を明することなく比較し、等しければ w 以下の V_i はなく、異なっていれば w 以下の V_i があると判定し、 w を変更して、最小値を決める。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000004226]

1. 変更年月日	1999年 7月15日
[変更理由]	住所変更
住 所	東京都千代田区大手町二丁目3番1号
氏 名	日本電信電話株式会社